(19) European Patent Office
Office européen des brevets

(11) EP 1 385 298 A1

(12) DEMANDE DE BREVET EUROPEEN

(43) Date de publication:
28.01.2004 Bulletin 2004/05

(51) Int Cl.[7]: **H04L 12/24**, G06F 17/22, G06F 17/21

(21) Numéro de dépôt: **03291511.8**

(22) Date de dépôt: **20.06.2003**

(84) Etats contractants désignés:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PT RO SE SI SK TR
Etats d'extension désignés:
AL LT LV MK

(30) Priorité: **25.07.2002 FR 0209437**

(71) Demandeur: **ALCATEL**
75008 Paris (FR)

(72) Inventeurs:
- **Chevanne, Michel**
  92140 Clamart (FR)
- **Lapraye, Bertrand**
  91190 Gif Sur Yvette (FR)
- **Drugmand, Philippe**
  92260 Fontenay aux Roses (FR)

(74) Mandataire: **Chaffraix, Sylvain et al**
Compagnie Financière Alcatel
Département de Propriété Industrielle,
5, rue Noel Pons
92734 Nanterre Cedex (FR)

(54) Dispositif et procédé de traitement de données pour la génération d'alarmes au sein d'un réseau de communications

(57) Un dispositif de traitement de données (1) comporte des moyens de traitement (4) capables de recevoir d'équipements (3) d'un réseau de communications des données primaires définissant des événements dans au moins un format primaire, et de délivrer à un dispositif de gestion du réseau (2) des données secondaires définissant des alarmes représentatives des événements, dans un format secondaire. Les moyens de traitement (4) comprennent un interpréteur (5) muni de règles de conversion, agencées sous forme de « scripts » associés aux différents formats primaires d'événement, et agencé pour convertir à l'aide de ces règles des données primaires, reçues dans l'un des formats primaires, en données secondaires dans le format secondaire interprétable par le dispositif de gestion (2).

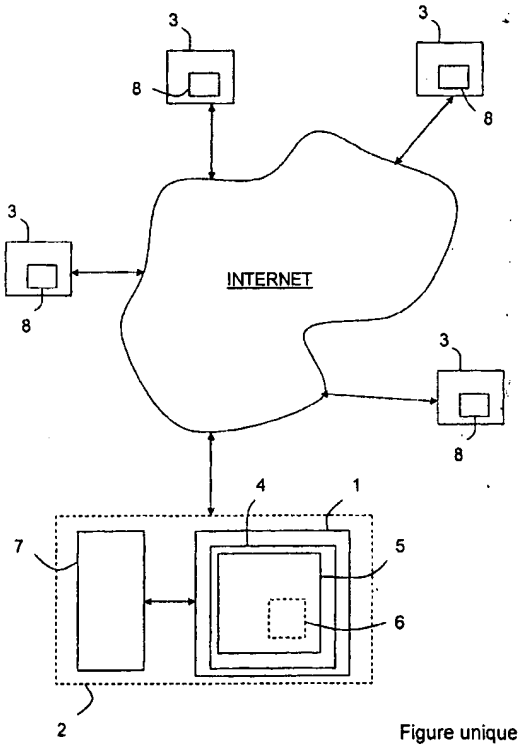

Figure unique

EP 1 385 298 A1

Description

[0001] L'invention concerne le domaine de l'échange de données entre équipements d'un réseau de communications, et plus particulièrement celui de la gestion d'événements survenant au sein desdits équipements.

[0002] Les réseaux de communications comportent généralement un dispositif de gestion de réseau (ou NMS pour « Network Management System ») censé prévenir l'opérateur lorsqu'un événement survient dans un équipement. Plus précisément, chaque fois que survient un événement au sein d'un équipement, ou dans un matériel supervisé par cet équipement, ce dernier délivre une notification représentative dudit événement. Cette notification, plus connue sous l'expression anglaise « Trap » lorsque le protocole de gestion du réseau est le protocole SNMP (pour « Simple Network Management Protocol » RFC 2571-2580), est constituée de données primaires agencées selon des formats (ou protocoles) primaires. A réception de ces données primaires le gestionnaire NMS analyse leur contenu, puis s'il reconnaît le premier format il génère une alarme définie par des données secondaires agencées selon un unique format (ou protocole) secondaire prédéfini.

[0003] Or, du fait de leur grande variété, les équipements d'un réseau utilisent fréquemment des formats primaires d'échange différents, difficiles, voire impossibles, à modifier. Par conséquent, les gestionnaires NMS ne peuvent reconnaître qu'une partie des notifications qu'ils reçoivent.

[0004] Pour tenter de remédier à cet inconvénient, il a été proposé d'équiper le gestionnaire NMS d'un module de traitement de données primaires reposant soit sur un outil de corrélation de formats, soit sur des codes de programmes, soit encore sur des fichiers de configuration. La première solution, reposant sur un outil de corrélation, met en oeuvre des traitements dont la lenteur est rédhibitoire. La deuxième solution, reposant sur des codes de programmes, nécessite des développements très coûteux. Enfin, la troisième solution n'est pas suffisamment souple pour convenir aux situations dans lesquelles les formats primaires sont assez différents, ce qui est généralement le cas. De plus, ces solutions ne permettent généralement pas de synchroniser ou resynchroniser l'état d'alarme des équipements au niveau du gestionnaire NMS. Par conséquent, aucune solution proposée n'est réellement satisfaisante.

[0005] L'invention a donc pour but de remédier à tout ou partie des inconvénients précités.

[0006] Elle propose à cet effet un dispositif de traitement de données comportant des moyens de traitement capables de recevoir d'équipements d'un réseau de communications des données primaires (ou notification) définissant des événements dans au moins un format primaire, et de délivrer à un dispositif de gestion du réseau (ou gestionnaire NMS) des données secondaires définissant des alarmes représentatives des événements, dans un format secondaire.

[0007] Ce dispositif se caractérise par le fait que ses moyens de traitement comprennent un interpréteur (ou « scripting engine ») muni de règles de conversion, agencées sous forme de « scripts » associés aux différents formats primaires d'événement, et agencé de manière à convertir à l'aide de ces règles des données primaires, reçues dans l'un des formats primaires, en données secondaires dans le format secondaire interprétable par le dispositif de gestion.

[0008] Préférentiellement, l'interpréteur est agencé pour effectuer ses conversions dans un format secondaire de fichier de configuration à l'aide d'un langage interprété. Plus préférentiellement encore, le format secondaire de fichier de configuration est un format de type XML (pour « eXtensible Markup Language » - version 1.0 recommandée par le W3C), et/ou le langage interprété est JavaScript (tel que défini par ECMA-262 ECMAScript: A general purpose, cross-platform programming language).

[0009] Egalement de préférence, lorsque les données primaires sont respectivement associées à des identifiants d'événements, comme par exemple des identifiants d'objets (ou OID pour « Object Identifier »), l'interpréteur peut être agencé de manière à stocker certaines au moins des règles de configuration en correspondance d'identifiants d'événements connus. Dans ce cas, l'interpréteur peut être également agencé de manière à stocker au moins une règle de conversion définissant un script par défaut destiné aux données primaires qui sont associées à un identifiant d'événement inconnu.

[0010] Avantageusement, l'interpréteur peut être agencé de manière à déduire de certaines données primaires reçues (ou notification) des paramètres d'alarme lui permettant de délivrer au dispositif de gestion une alarme paramétrée. Dans ce cas, les alarmes peuvent être paramétrées par des valeurs « codées en dur » et/ou extraites des données primaires, et/ou des valeurs extraites d'un équipement. Dans cette dernière hypothèse, l'interpréteur doit être agencé pour extraire d'un équipement du réseau, dont l'état d'alarme est inconnu (de préférence de sa base d'informations de gestion ou MIB (pour « Management Information Base »)), des informations choisies représentatives de son état d'alarme, puis simuler l'émission de données primaires (ou notification) représentatives de ces informations d'état, de manière à générer une alarme destinée à signaler au dispositif de gestion l'état d'alarme de l'équipement.

[0011] Par ailleurs, les données primaires sont préférentiellement reçues dans des formats primaires de type SNMP (protocole de gestion de réseau Internet).

[0012] L'invention porte également sur un dispositif de gestion de réseau (ou gestionnaire NMS) comprenant un dispositif de traitement du type de celui présenté ci-avant.

[0013] L'invention porte en outre sur un procédé de traitement de données, dans lequel, à réception de données primaires (ou notification) transmises par des équi-

pements d'un réseau de communications et définissant des événements dans au moins un format primaire, on délivre à un dispositif de gestion du réseau (ou gestionnaire NMS) des données secondaires définissant des alarmes représentatives des événements, dans un format secondaire.

[0014] Ce procédé se caractérise par le fait que son étape de génération consiste à convertir à l'aide de règles de conversion, agencées sous forme de « scripts » associés aux différents formats primaires d'événement, des données primaires, reçues dans l'un des formats primaires, en données secondaires dans le format secondaire interprétable par le dispositif de gestion.

[0015] Le procédé selon l'invention pourra comporter de nombreuses caractéristiques complémentaires qui pourront être prises séparément et/ou en combinaison, et en particulier:

- on peut procéder à la conversion dans un format secondaire de fichier de configuration à l'aide d'un langage interprété. Il est alors préférable que le format secondaire du fichier de configuration soit un format de type XML, et/ou que le langage interprété soit JavaScript ;
- en présence de données primaires associées respectivement à des identifiants d'événements, on peut associer certaines au moins des règles de conversion à des identifiants d'événements connus. Dans ce cas, il est avantageux que l'une au moins des règles de conversion soit définie par un script par défaut destiné à des données primaires associées à un identifiant d'événement inconnu ;
- on peut déduire de certaines données primaires reçues des paramètres d'alarme, de manière à délivrer au dispositif de gestion une alarme paramétrée, par exemple par des valeurs « codées en dur » et/ou des valeurs extraites des données primaires et/ou des valeurs extraites d'un équipement ;
- on peut extraire d'un équipement du réseau, dont l'état d'alarme est inconnu, des informations choisies représentatives de son état d'alarme, puis simuler l'émission de données primaires représentatives de ces informations d'état, de manière à générer une alarme destinée à signaler au dispositif de gestion l'état d'alarme de l'équipement. Cette extraction s'effectue préférentiellement dans la base d'informations de gestion de l'équipement concerné ;
- les données primaires sont préférentiellement reçues dans des formats primaires de type SNMP.

[0016] L'invention peut notamment être mise en oeuvre dans toutes les technologies réseaux devant être gérées, et notamment dans les réseaux de transmission (par exemple de type WDM, SONET, SDH), de données (par exemple de type Internet-IP ou ATM) ou de voix (par exemple de type classique, mobile ou NGN).

[0017] D'autres caractéristiques et avantages de l'invention apparaîtront à l'examen de la description détaillée ci-après, et de l'unique figure annexée qui illustre de façon schématique un exemple de réalisation d'un dispositif selon l'invention implanté dans un gestionnaire NMS d'un réseau de communications. Cette figure est, pour l'essentiel, de caractère certain. En conséquence, elle pourra non seulement servir à compléter l'invention, mais aussi contribuer à sa définition, le cas échéant.

[0018] Le dispositif de traitement 1 selon l'invention est destiné à alimenter en alarmes un gestionnaire NMS (pour « Network Management System ») 2 d'un réseau de communications, par exemple de type Internet. Dans l'exemple illustré sur l'unique figure, ce dispositif 1 est implanté dans le gestionnaire NMS 2, mais il pourrait être implanté dans un boîtier externe, couplé audit gestionnaire NMS.

[0019] Le réseau de communications comporte une multiplicité d'équipements de réseau 3, comme par exemple des serveurs, des terminaux, des commutateurs ou des routeurs, pouvant échanger des données selon un protocole de gestion de réseau avec le gestionnaire NMS 2.

[0020] Dans ce qui suit, on considère à titre d'exemple non limitatif que le réseau de communications est de type Internet (IP) et que le protocole de gestion du réseau est le protocole SNMP (pour « Simple Network Management Protocol » RFC 2571-2580). Bien entendu, l'invention s'applique à d'autres types de réseau, comme par exemple aux réseaux de transmission de type WDM, SONET ou SDH, de données de type ATM, ou de voix de type classique, mobile ou NGN, et à d'autres protocoles de gestion de réseau, comme par exemple TL1 ou CORBA. Les équipements 3 du réseau sont agencés pour délivrer au gestionnaire NMS 2 des notifications (ou messages), ici de type « Trap », définies par des données primaires agencées selon un format (ou protocole) primaire, ici de type SNMP, chaque fois que survient un événement en leur sein, ou dans un équipement ou matériel qu'ils contrôlent. Les données primaires d'une notification définissent par conséquent un événement survenu dans un équipement 3. Une multiplicité de formats primaires différents peut coexister au sein du réseau. Par ailleurs, chaque notification est préférentiellement associée à un identifiant représentatif d'un type d'événement.

[0021] Le dispositif de traitement 1 comprend un module de traitement 4 comportant un interpréteur (ou « scripting engine ») 5 disposant d'une multiplicité de règles de conversion agencées sous la forme de « scripts » associés à une multiplicité de formats primaires d'événement différents.

[0022] Plus précisément, à chaque format primaire correspond un script particulier (ou règle(s) de conversion), préférentiellement stocké dans une mémoire 6 en correspondance de l'un des identifiants d'événements contenus dans les notifications (ou Traps). Il est égale-

ment préférable de prévoir au moins un script par défaut pour traiter (ou initier le traitement) les données primaires agencées selon un format primaire qui est associé à un identifiant d'événement inconnu.

[0023] Ainsi, lorsqu'un interpréteur 5 reçoit une notification (ou Trap), il en extrait l'identifiant d'événement et détermine la règle de configuration (ou script) stockée qui lui correspond. Il peut alors appliquer ce script (ou règle) aux données primaires définissant la notification, de manière à générer une alarme définie par des données secondaires agencées dans un langage interprété et selon un unique format secondaire interprétable par un module de contrôle 7 du gestionnaire NMS 2. En d'autres termes, les données primaires reçues, agencées selon un format primaire et représentatives d'un événement, sont « converties » en données secondaires agencées selon un format secondaire et dans un langage interprété.

[0024] A réception d'une telle alarme, le module de contrôle 7 du gestionnaire NMS 2 peut alors provoquer l'affichage de l'alarme sur un écran de contrôle dudit gestionnaire NMS et/ou décider d'action(s) à entreprendre dans le réseau pour tenir compte de l'alarme et/ou remédier à sa cause.

[0025] L'interpréteur 5 est agencé, à réception de données primaires, pour générer, à l'aide du script qui correspond aux données primaires reçues, une alarme définie par des données secondaires. Dans un mode de réalisation préférentiel, ces données secondaires sont agencées sous la forme d'un fichier de configuration d'alarme selon un format (ou protocole) secondaire, de préférence de type XML (pour « eXtensible Markup Language »), et dans un langage interprété (ou « scripting language »), de préférence de type JavaScript (tel que défini par ECMA-262 ECMAScript : A general purpose, cross-platform programming language). Plus préférentiellement encore, on choisit la version 1.0, du format XML recommandée par W3C.

[0026] Bien entendu, d'autres langages interprétés (ou « scripting languages ») et d'autres formats secondaires pourraient être envisagés. Ainsi, XML peut être remplacé par des formats textes propriétaires. De même, le langage JavaScript des scripts peut être remplacé, par exemple, par VisualBasic, TCL, Perl ou encore Python.

[0027] Dans cet exemple, l'identifiant d'événement, permettant à l'interpréteur 5 de déterminer le script correspondant au format primaire des données primaires reçues, est préférentiellement de type OID (« Object Identifier »- identifiant de type simple ASN.1 permettant d'identifier un objet tel qu'un événement), dans la mesure où le langage interprété, utilisé par l'interpréteur 5 pour générer les fichiers de configuration (données secondaires), est JavaScript.

[0028] La syntaxe utilisée pour générer les fichiers de configuration d'alarme (ou données secondaires) est donc ici une combinaison de XML et de JavaScript. Plus précisément, d'une première part, la structure générale du fichier est de type XML, d'une deuxième part, les données secondaires, définissant l'alarme associée à une notification OID reçue, sont toujours encadrées par deux blocs (ou « tags ») XML, d'une troisième part, chaque champ de l'alarme possède une unique entrée, et d'une quatrième part, chaque entrée de l'alarme est soit une constante, soit une expression JavaScript.

[0029] Ainsi, lorsque toutes les entrées de l'alarme sont des constantes, le fichier de configuration d'alarme est principalement de type XML. Par exemple, il se présente sous la forme <SEVERITY>Critical</SEVERITY>. Lorsque certaines au moins des entrées de l'alarme sont des expressions JavaScript, un maximum de souplesse peut être obtenu. Le fichier se présente alors, par exemple, sous la forme <SEVERITY> (trapget(« 1.2.3.4 »)==2) ? Critical : Major</SEVERITY>.

[0030] Certains champs de l'alarme générée peuvent être optionnels ou présenter une valeur par défaut.

[0031] Grâce aux scripts, il est possible de tirer pleinement partie des informations contenues dans les données primaires qui constituent les notifications reçues. De nombreux traitements, notamment logiques et/ou calculatoires, peuvent être ainsi appliqués aux paramètres qui définissent les événements signalés par les équipements 3 du réseau. Par conséquent, l'interpréteur 5 peut non seulement générer une alarme représentative d'un événement, mais également accompagner cette alarme de paramètres (ou de valeurs de paramètres) susceptibles d'en faciliter le traitement au niveau du gestionnaire NMS 2.

[0032] Les alarmes peuvent ainsi être paramétrées par des valeurs « codées en dur » et/ou extraites de la notification (ou Trap) et/ou extraites d'un équipement dont on a reçu une notification (ou Trap).

[0033] Afin de mettre en oeuvre cette troisième possibilité, l'interpréteur 5 doit être agencé de manière à adresser à un équipement, dont il a éventuellement reçu des données primaires représentatives d'un état d'alarme inconnu, un message requérant de sa part certaines informations susceptibles de permettre la détermination dudit état d'alarme. Généralement, ces informations sont contenues dans la base d'informations de gestion 8 (ou MIB pour « Management Information Base ») de l'équipement 3.

[0034] Grâce à cet agencement lui permettant d'extraire des informations d'un équipement 3 distant, et notamment de sa MIB 8, le dispositif selon l'invention 1 peut assurer une fonction de synchronisation et resynchronisation de l'état d'alarme de chaque équipement. En effet, chaque fois que le gestionnaire NMS du réseau 2 (ou son dispositif de traitement 1) est redémarré ou déconnecté du reste du réseau, par exemple en cas de panne ou d'intervention de maintenance, il doit être, d'une part, resynchronisé par rapport aux états d'alarmes respectifs des équipements 3 du réseau qui étaient présents au moment de sa déconnexion, lesquels états ont pu évoluer, et d'autre part, synchronisé par rapport aux états d'alarmes respectifs des nouveaux équipe-

ments 3 du réseau, lesquels états lui sont inconnus. Il en va de même chaque fois qu'un nouvel équipement 3 se connecte au réseau ou qu'un ancien équipement se reconnecte au réseau.

[0035] Cette fonction peut être assurée par une ou plusieurs règles, par exemple stockées dans la mémoire 6, soit automatiquement lors de chaque mise en fonctionnement et/ou chaque fois que l'interpréteur 5 est averti d'une (re)connexion par le module de contrôle 7 du gestionnaire NMS 2 du réseau, soit semi-automatiquement chaque fois que la personne responsable de la gestion du réseau en donne l'ordre à l'interpréteur 5.

[0036] La ou les règles de (re)synchronisation sont agencées pour examiner le contenu de la MIB du ou des équipements 3 désignés, de manière à extraire les informations (paramètre(s) ou valeur(s) de paramètre(s)) définissant leur(s) état(s) d'alarme. Mais, ces règles peuvent également servir à vérifier ou contrôler la valeur d'un ou plusieurs paramètres. Comme indiqué ci-dessus, dans certaines situations tous les équipements du réseau, qui dialoguent avec le gestionnaire NMS 2, peuvent faire l'objet d'un examen à l'aide des règles de (re) synchronisation.

[0037] La ou les règles de (re)synchronisation peuvent être agencées de manière à simuler l'émission d'une notification (ou Trap) à l'intérieur du gestionnaire NMS 2. Plus précisément, elles indiquent les notifications (ou Traps) que l'équipement 3 aurait dû envoyer pour passer d'un état sans alarme à son état en cours. Ces notifications (ou Traps) simulées font ensuite l'objet d'une conversion semblable à celle appliquée aux notifications réelles.

[0038] Le module de traitement 4 du dispositif 1, et son interpréteur 5, peuvent être respectivement réalisés sous la forme de circuits électroniques, de modules logiciels (ou informatiques), ou d'une combinaison de circuits et de logiciels.

[0039] L'invention offre également un procédé de traitement de données, dans lequel, à réception de données primaires transmises par des équipements 3 d'un réseau de communications et définissant des événements dans au moins un format primaire, on délivre à un dispositif de gestion du réseau 2 (ou gestionnaire NMS) des données secondaires qui définissent des alarmes représentatives de ces événements, dans un format secondaire.

[0040] Celui-ci peut être mis en oeuvre à l'aide du dispositif de traitement présenté ci-avant. La fonction principale et les sous-fonctions optionnelles assurées par les étapes de ce procédé étant sensiblement identiques à celles assurées par les différents moyens constituant le dispositif de traitement 1, seule sera résumée ci-après l'étape mettant en oeuvre la fonction principale du procédé selon l'invention.

[0041] Ce procédé se caractérise par le fait que son étape de génération consiste à convertir à l'aide de règles de conversion, agencées sous forme de « scripts » associés aux différents formats primaires d'événement, des données primaires, reçues dans l'un des formats primaires, en données secondaires dans le format secondaire interprétable par le dispositif de gestion 2.

[0042] Grâce à l'invention, il n'est plus nécessaire de recourir à la programmation, ce qui permet de réduire les coûts de développement. De plus, les scripts procurent une grande souplesse d'utilisation et une grande rapidité de traitement (plusieurs dizaines de notifications (ou Traps) par seconde), et permettent une adaptation rapide à tous les types de formats primaires. En outre, l'invention permet une (re)synchronisation.

[0043] L'invention ne se limite pas aux modes de réalisation de procédé et dispositifs décrits ci-avant, seulement à titre d'exemple, mais elle englobe toutes les variantes que pourra envisager l'homme de l'art dans le cadre des revendications ci-après.

Revendications

1. Dispositif de traitement de données (1) comportant des moyens de traitement (4) propres à recevoir d'équipements (3) d'un réseau de communications des données primaires définissant des événements dans au moins un format primaire, et à délivrer à un dispositif de gestion dudit réseau (2) des données secondaires définissant des alarmes représentatives desdits événements, dans un format secondaire, **caractérisé en ce que** lesdits moyens de traitement (4) comprennent un interpréteur (5) muni de règles de conversion, agencées sous forme de « scripts » associés aux différents formats primaires d'événement, et agencé pour convertir à l'aide desdites règles des données primaires, reçues dans l'un desdits formats primaires, en données secondaires dans ledit format secondaire interprétable par ledit dispositif de gestion (2).

2. Dispositif selon la revendication 1, **caractérisé en ce que** ledit interpréteur (5) est agencé pour effectuer lesdites conversions dans un format secondaire de fichier de configuration à l'aide d'un langage interprété.

3. Dispositif selon la revendication 2, **caractérisé en ce que** ledit format secondaire de fichier de configuration est un format choisi dans un groupe comprenant XML et les formats textes propriétaires.

4. Dispositif selon l'une des revendications 2 et 3, **caractérisé en ce que** ledit langage interprété est choisi dans un groupe comprenant au moins JavaScript, VisualBasic, TCL, Perl et Python.

5. Dispositif selon l'une des revendications 1 à 4, **caractérisé en ce que**, en présence de données primaires associées respectivement à des identifiants d'événements, ledit interpréteur (5) est agencé pour

stocker certaines au moins desdites règles en correspondance d'identifiants d'événements connus.

6. Dispositif selon la revendication 5, **caractérisé en ce que** ledit interpréteur (5) est agencé pour stocker au moins une règle de conversion définissant un script par défaut destiné aux données primaires associées à un identifiant d'événement inconnu.

7. Dispositif selon l'une des revendications 1 à 6, **caractérisé en ce que** ledit interpréteur (5) est agencé pour déduire de certaines données primaires reçues des paramètres d'alarme, de manière à délivrer audit dispositif de gestion (2) une alarme paramétrée.

8. Dispositif selon la revendication 7, **caractérisé en ce que** ledit interpréteur (5) est agencé pour délivrer au dit dispositif de gestion (2) des alarmes paramétrées par des valeurs « codées en dur ».

9. Dispositif selon l'une des revendications 7 et 8, **caractérisé en ce que** ledit interpréteur (5) est agencé pour délivrer audit dispositif de gestion (2) des alarmes paramétrées par des valeurs extraites desdites données primaires.

10. Dispositif selon l'une des revendications 1 à 9, **caractérisé en ce que**, lorsque l'état d'alarme d'un équipement (3) du réseau est inconnu, ledit interpréteur (5) est agencé pour extraire dudit équipement (3) des informations choisies représentatives dudit état d'alarme, puis simuler l'émission de données primaires représentatives desdites informations d'état, de manière à générer une alarme destinée à signaler au dispositif de gestion (2) l'état d'alarme dudit équipement (3).

11. Dispositif selon la revendication 10 en combinaison avec l'une des revendications 7 à 9, **caractérisé en ce que** ledit interpréteur (5) est agencé pour délivrer audit dispositif de gestion (2) des alarmes paramétrées par des valeurs extraites de l'équipement duquel il a reçu des données primaires.

12. Dispositif selon l'une des revendications 10 et 11, **caractérisé en ce que** ledit interpréteur (5) est agencé pour extraire lesdites informations ou valeurs d'une base d'informations de gestion (8) de l'équipement concerné.

13. Dispositif selon l'une des revendications 1 à 12, **caractérisé en ce que** lesdites données primaires sont reçues dans des formats primaires de type SNMP.

14. Dispositif de gestion de réseau (2), **caractérisé en ce qu'**il comprend un dispositif de traitement (1) selon l'une des revendications précédentes.

15. Procédé de traitement de données, dans lequel, à réception de données primaires transmises par des équipements (3) d'un réseau de communications et définissant des événements dans au moins un format primaire, on délivre à un dispositif de gestion du réseau (2) des données secondaires définissant des alarmes représentatives desdits événements, dans un format secondaire, **caractérisé en ce que** ladite génération consiste à convertir à l'aide de règles de conversion, agencées sous forme de « scripts » associés aux différents formats primaires d'événement, des données primaires, reçues dans l'un desdits formats primaires, en données secondaires dans ledit format secondaire interprétable par ledit dispositif de gestion (2).

16. Procédé selon la revendication 15, **caractérisé en ce que** l'on procède à la conversion dans un format secondaire de fichier de configuration à l'aide d'un langage interprété.

17. Dispositif selon la revendication 16, **caractérisé en ce que** ledit format secondaire de fichier de configuration est un format choisi dans un groupe comprenant XML et les formats textes propriétaires.

18. Dispositif selon l'une des revendications 16 et 17, **caractérisé en ce que** ledit langage interprété est choisi dans un groupe comprenant au moins JavaScript, VisualBasic, TCL, Perl et Python.

19. Procédé selon l'une des revendications 15 à 18, **caractérisé en ce que**, en présence de données primaires associées respectivement à des identifiants d'événements, on associe certaines au moins desdites règles de conversion à des identifiants d'événements connus.

20. Procédé selon la revendication 19, **caractérisé en ce que** l'une au moins desdites règles de conversion définit un script par défaut destiné à des données primaires associées à un identifiant d'événement inconnu.

21. Procédé selon l'une des revendications 15 à 20, **caractérisé en ce que** l'on déduit de certaines données primaires reçues des paramètres d'alarme, de manière à délivrer audit dispositif de gestion (2) une alarme paramétrée.

22. Procédé selon la revendication 21, **caractérisé en ce que** l'on délivre audit dispositif de gestion (2) des alarmes paramétrées par des valeurs « codées en dur ».

23. Procédé selon l'une des revendications 21 et 22,

caractérisé en ce que l'on délivre audit dispositif de gestion (2) des alarmes paramétrées par des valeurs extraites desdites données primaires.

24. Procédé selon l'une des revendications 15 à 23, **caractérisé en ce que**, lorsque l'état d'alarme d'un équipement (3) du réseau est inconnu, on extrait dudit équipement (3) des informations choisies représentatives dudit état d'alarme, puis on simule l'émission de données primaires représentatives desdites informations d'état, de manière à générer une alarme destinée à signaler au dispositif de gestion (2) l'état d'alarme dudit équipement (3).

25. Procédé selon la revendication 24 en combinaison avec l'une des revendications 21 à 23, **caractérisé en ce que** l'on délivre audit dispositif de gestion (2) des alarmes paramétrées par des valeurs extraites de l'équipement (3) duquel il a reçu des données primaires.

26. Procédé selon l'une des revendications 24 et 25, **caractérisé en ce que** l'on extrait lesdites informations ou valeurs d'une base d'informations de gestion (8) de l'équipement (3) concerné.

27. Procédé selon l'une des revendications 15 à 26, **caractérisé en ce que** lesdites données primaires sont reçues dans des formats primaires de type SNMP.

28. Utilisation des procédé, dispositif de traitement (1) et dispositif de gestion (2) selon l'une des revendications précédentes dans les technologies réseaux devant être gérées.

29. Utilisation selon la revendication 28, **caractérisé en ce que** lesdites technologies réseaux sont choisies dans un groupe comprenant les réseaux de transmission, en particulier de type WDM, SONET et SDH, de données, en particulier de type Internet-IP et ATM, et de voix, en particulier de type classique, mobile et NGN.

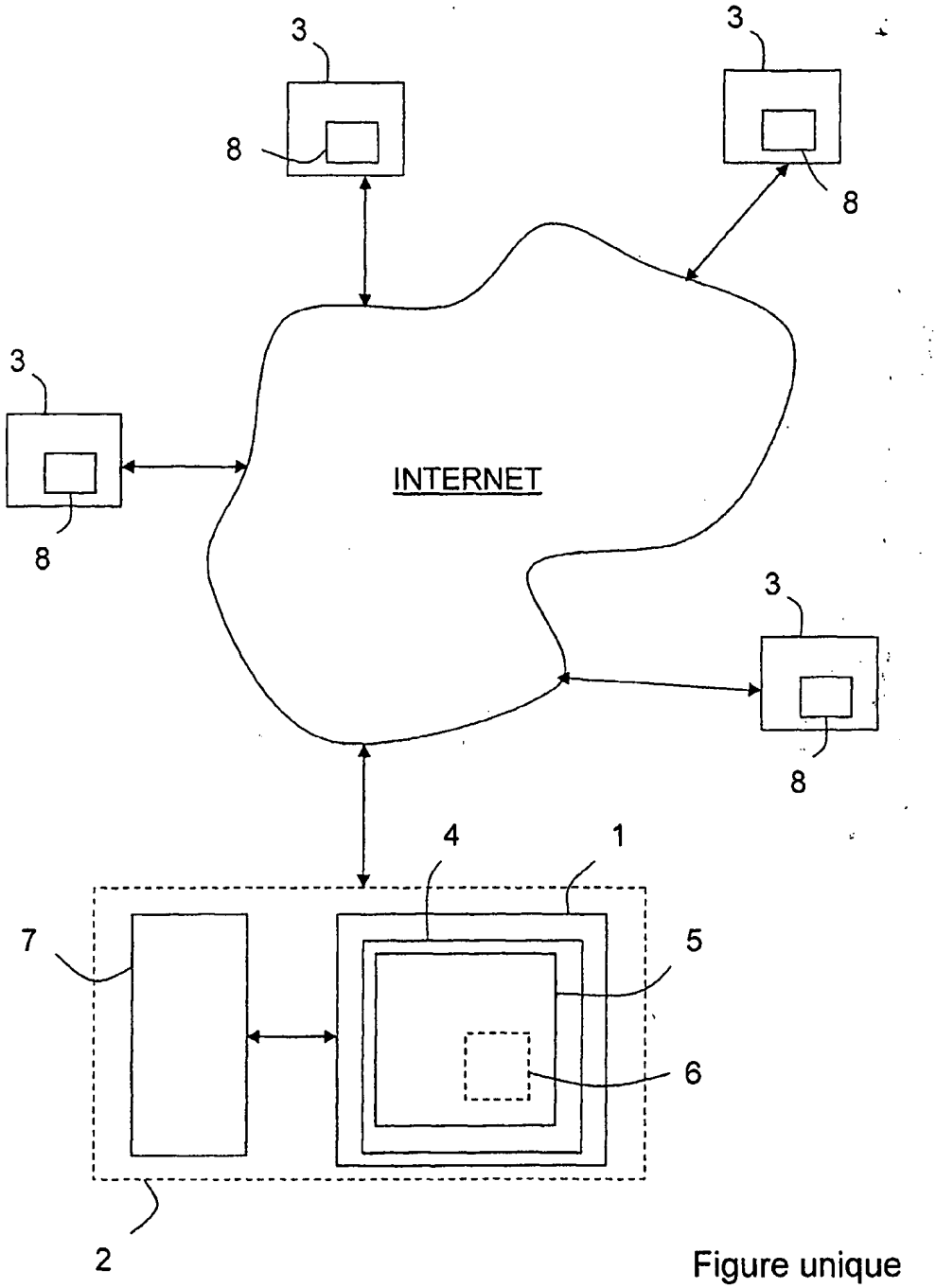

Figure unique

Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande
EP 03 29 1511

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (Int.Cl.7)
Y	US 5 202 977 A (PASETES JR EMMANUEL K ET AL) 13 avril 1993 (1993-04-13) * abrégé * * colonne 16, ligne 18 - colonne 22, ligne 36 *	1,2,5, 14-16, 19,28	H04L12/24 G06F17/22 G06F17/21
A	* colonne 7, ligne 5 - colonne 8, ligne 55 *	3,4, 6-13,17, 18, 20-27,29	

Y	US 5 987 513 A (RAVINDRAN VIJI KAKKATTU ET AL) 16 novembre 1999 (1999-11-16)	1,2,5, 14-16, 19,28	
A	* abrégé *	3,4, 6-13,17, 18, 20-27,29	
	* colonne 2, ligne 47 - colonne 5, ligne 14 * * colonne 24, ligne 65 - colonne 26, ligne 6 *		DOMAINES TECHNIQUES RECHERCHES (Int.Cl.7)
	---		H04L G06F
A	JAKOBSON G ET AL: "GRACE: Building Next Generation Event Correlation Services" IEEE, XP010376718 * abrégé * * page 706, alinéa 4.1 - page 709, alinéa 5. *	1-29	

Le présent rapport a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
LA HAYE	1 septembre 2003	Stergiou, C

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C02)

ANNEXE AU RAPPORT DE RECHERCHE EUROPEENNE RELATIF A LA DEMANDE DE BREVET EUROPEEN NO. EP 03 29 1511

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche européenne visé ci-dessus.
Lesdits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets.

01-09-2003

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 5202977 A	13-04-1993	AT 161342 T	15-01-1998
		AU 8314691 A	04-02-1992
		DE 69128483 D1	29-01-1998
		EP 0553098 A1	04-08-1993
		WO 9201251 A1	23-01-1992
US 5987513 A	16-11-1999	AUCUN	

EPO FORM P0460

Pour tout renseignement concernant cette annexe : voir Journal Officiel de l'Office européen des brevets, No.12/82